Mohamed Mahmoud Zakzouk

Information Security Engineer

About

Mohamed is a Information Security Engineer, who trying anything related to computer security, Software, Hardware, Penetration Testing, Red-teaming, ... etc. The knowledge in Electronics and Communications gives him an advantage in hardware and radio hacking more than others in the field. After spending nearly three years in the Egyptian Armed Forces as a reserve officer. Became able to work with different situations and deal with difficult situations. Won the unit's best officer award three times in a row during his military service.

Contact

Mobile:
+201007277213

Email:
mohamedm.zakzouk@gmail.com

Website:
math3ng.github.io

Linkedin:
mohamed-zakzouk

Address:
El-Behira, Egypt

PROFESSIONAL SKILLS

- Penetration Testing
- Active Directory
- Scripting
- Privilege Escalation
- Pivot
- OWASP TOP 10
- AWS Cloud
- IOT Hacking
- SIEM Solutions
- Splunk and IBM QRadar

SOFT SKILLS

- **Leadership**

- Gained from years in Egyptian Army

- **Public speaking**

- Was a speaker in some events.

- **Planning**

- Project manager in civil work in two events.

- **Communication**

- Bring on a partner and speakers during civil work more than once.

- **Embraces teamwork**

- Gained from civil work and Egyptian Army.

- **Dealing with difficult situations**

- Through multiple situations in civil work and military service.

- **Analytical and Problem-solving**

- During multiple situations in military service

Education

B.S Electronics and Communications **2014-2019**
Alexandria University

Graduation Project: IOT (Smart City Model)
Graduation Project Grade: Excellent
Tasks:
1. Working on mobile app using xamarin.
2. Making the app available on cloud using azure.
3. Creating a Face Recognition with python and open CV.
4. Implement the Face Recognition with raspberry pi.
5. Dealing with Arduino in some tasks.

Programming

- Python
- Bash
- Powershell
- PHP
- Assembly

Programming Projects

- Face Recognition sample using openCV
- Block-chain sample
- Round robin algorithm
- Deadlock detection
- Image co-ordinates
- RC4

Self-Study Course

- 1. OSCP
- 2. OSEP
- 3. CRTP
- 3. PTX
- 4. CCNA Routing&Switching
- 5. CCNA Security
- 6. Linux

CTFs

Tryhackme:
Rank: God (maximum rank)
Completed more than 150 rooms.

Hackthebox:
Rank: Hacker
Rooted more than 50 machines.

Military Service

Status: **completed**

Role: **Reserve Officer**

Date: **Oct-2019 : Apr-2022**

Languages

English:
Professional working proficiency

Arabic:
Native

Certifications

ThrowBack
TryHackMe | December 2021

Throwback is an Active Directory (AD) lab that teaches the fundamentals and core concepts of attacking a Windows network. The network simulates a realistic corporate environment such as following attacks:

- Phishing & OSINT
- Offensive Powershell
- Active Directory Basics
- Kerberos Abuse
- Custom Malicious Macros
- Active Directory Enumeration & Exploitation
- Attacking Mail Servers
- Firewall Pivoting
- C2 Frameworks
- Abusing Cross-Domain Trusts

Jr. Penetration tester
TryHackMe | December 2021

This learning path covers the core technical skills that will allow you to perform security assessments against web applications and enterprise infrastructure.

- Introduction to Pentesting
- Introduction to Web hacking
- Burp Suite
- Network Security
- Vulnerability Research
- Metasploit
- Privilege Escalation

Offensive Pentesting
TryHackMe | November 2021

The aim of this path is to make you ready for real world penetration testing by teaching you how to use industry standard tools along with a methodology to find vulnerabilities in machines.

- Advanced Exploitation
- Buffer Overflow Exploitation
- Active Directory

Cyber Defense
TryHackMe | November 2021

The Cyber Defense path aims to give a broad introduction to the different areas necessary to detect and respond to threats such as:

- Threat and Vulnerability Management
- Security Operations and Monitoring
- Threat Emulation
- Incident Response & Forensics
- Malware Analysis and Reverse Engineering

Preference

All proofs are on my website: https://math3ng.github.io/